ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Отчет об оценке по функциональной безопасности № ФБ01.0069/ФБ от 13.10.2023

Оборудование: Повторители сигналов искробезопасные ЛПА-310, Барьеры искробезопасности ЛПА-340, Преобразователи температуры вторичные искробезопасные ЛПА-350

Изготовитель: Общество с ограниченной ответственностью "Ленпромавтоматика"

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Оглавление

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

1. Заявитель на сертификацию

Общество с ограниченной ответственностью "Ленпромавтоматика".

Место нахождения (адрес юридического лица): 190020, Россия, город Санкт-Петербург, вн.тер.г. муниципальный округ Екатерингофский, набережная Бумажного канала, дом 18, литера А, помещение 10-Н.

2. Изготовитель продукции

Общество с ограниченной ответственностью "Ленпромавтоматика".

Место нахождения (адрес юридического лица) и адрес места осуществления деятельности: 190020, Россия, город Санкт-Петербург, вн.тер.г. муниципальный округ Екатерингофский, набережная Бумажного канала, дом 18, литера А, помещение 10-Н.

3. Наименование продукции

Повторители сигналов искробезопасные ЛПА-310, Барьеры искробезопасности ЛПА-340, Преобразователи температуры вторичные искробезопасные ЛПА-350.

4. Перечень стандартов на соответствие которым проведена оценка функциональной безопасности

№	Обозначение стандарта	Наименование стандарта
1	ГОСТ Р МЭК 61508-1-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования
2	ГОСТ Р МЭК 61508-2-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам
3	ГОСТ IEC 61508-3-2018	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению
При составлении отчета учтены положения связанных стандартов		
5	ГОСТ Р МЭК 61508-4-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения
6	ГОСТ Р МЭК 61508-5-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
7	ГОСТ Р МЭК 61508-6-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3
8	ГОСТ Р МЭК 61508-7-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

5. Перечень рассмотренной документации

№	Обозначение документа	Наименование документа
ЛПА 310:		
1.	ТУ 27.12.23-017-13898149-2020	Технические условия
2.	ОЛПА-21.018.28 ПС	Паспорт
3.	ОЛПА-21.018.28 РЭ	Руководство по эксплуатации
4.	ОЛПА-21.018.28 СБ	Чертёж
5.	ОЛПА-31.014.01 СБ	Чертёж
6.	ОЛПА-31.014.02 СБ	Чертёж
7.	ОЛПА-34.001.08 СБ	Чертёж
8.	ОЛПА-34.001.09 СБ	Чертёж
9.	ОЛПА-41.001.40	Печатная плата
10	ОЛПА-41.001.43	Печатная плата
11	ОЛПА-51.001.49 ПЭ3	Перечень компонентов
12	ОЛПА-51.001.49 СБ	Сборочный чертёж
13	ОЛПА-51.001.49 Э3	Схема электрическая
14	ОЛПА-51.001.49-01 ПЭ3	Перечень компонентов
15	ОЛПА-51.001.49-01 СБ	Чертёж
16	ОЛПА-51.001.49-01 Э3	Схема электрическая
17	ОЛПА-51.001.49-02 ПЭ3	Перечень компонентов
18	ОЛПА-51.001.49-02 СБ	Чертёж
19	ОЛПА-51.001.49-02 Э3	Схема электрическая
20	ОЛПА-61.004.01 СБ	Чертёж
21	ОЛПА-61.005.01 СБ	Чертёж
22	TPH-ER9.5-N87-01 СБ	Чертёж
23	-	FMEDA анализ
24	-	Руководство по функциональной безопасности
ЛПА 340:		
25	ОЛПА-51.001.51-02 Э3	Схема электрическая
26	ОЛПА-51.001.51-03 ПЭ3	Перечень компонентов
27	ОЛПА-51.001.51-03 СБ	Чертёж
28	ОЛПА-51.001.51-03 Э3	Схема электрическая
29	ОЛПА-41.001.44	Печатная плата
30	ТУ 27.12.23-019-13898149-2021	Технические условия
31	ОЛПА-21.018.29 ГЧ	Чертёж
32	ОЛПА-21.018.29 ПЗ	Пояснительная записка
33	ОЛПА-21.018.29 ПС	Паспорт
34	ОЛПА-21.018.29 РЭ	Руководство по эксплуатации
35	ОЛПА-21.018.29 СБ	Чертёж
36	ОЛПА-31.014.04 СБ	Чертёж
37	ОЛПА-34.001.13 СБ	Чертёж
38	ОЛПА-41.001.41	Печатная плата
39	ОЛПА-51.001.51 ПЭ3	Перечень компонентов
40	ОЛПА-51.001.51 СБ	Чертёж
41	ОЛПА-51.001.51 Э3	Схема электрическая
42	ОЛПА-51.001.51-01 ПЭ3	Перечень компонентов
43	ОЛПА-51.001.51-01 СБ	Чертёж
44	ОЛПА-51.001.51-01 Э3	Схема электрическая
45	ОЛПА-51.001.51-02 ПЭ3	Перечень компонентов
46	ОЛПА-51.001.51-02 СБ	Чертёж
47	-	FMEDA анализ
48	-	Руководство по функциональной безопасности
ЛПА 350:		
49	ОЛПА-21.018.30 СБ	Чертёж
50	ОЛПА-51.001.50-02 ПЭ3	Перечень элементов
51	ОЛПА-51.001.50-02 СБ	Чертёж
52	ОЛПА-51.001.50-02 Э3	Схема электрическая
53	ОЛПА-51.001.50-03 ПЭ3	Перечень элементов
54	ОЛПА-51.001.50-03 СБ	Чертёж
55	ОЛПА-51.001.50-03 Э3	Схема электрическая

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

56	ОЛПА-51.001.50-08 ПЭ3	Перечень элементов
57	ОЛПА-51.001.50-08 СБ	Чертёж
58	ОЛПА-51.001.50-08 Э3	Схема электрическая
59	ОЛПА-51.001.50-09 ПЭ3	Перечень элементов
60	ОЛПА-51.001.50-09 СБ	Чертёж
61	ОЛПА-51.001.50-09 Э3	Схема электрическая
62	ОЛПА-51.001.50 ПЭ3	Перечень элементов
63	ОЛПА-51.001.50 СБ	Чертёж
64	ОЛПА-51.001.50 Э3	Схема электрическая
65	ОЛПА-51.001.50-01 ПЭ3	Перечень элементов
66	ОЛПА-51.001.50-01 СБ	Чертёж
67	ОЛПА-41.001.45	Печатная плата
68	ОЛПА-31.014.03 СБ	Чертёж
69	ОЛПА-21.018.30 ПС	Паспорт
70	ОЛПА-41.001.44	Печатная плата
71	ОЛПА-21.018.30 РЭ	Руководство по эксплуатации
72	ТУ 27.12.23-018-13898149-2021	Технические условия
73	ОЛПА-41.001.44	Печатная плата
74	ОЛПА-34.001.10 СБ	Чертёж
75	ОЛПА-34.001.11 СБ	Чертёж
76	-	FMEDA-анализ
77	-	Руководство по функциональной безопасности
78	-	Сведения о применяемом ПО
Общее:		
79	ЕАЭС RU C-RU.НВ07.В.00487/21	Сертификат соответствия требованиям ТР ТС 012/2011
80	-	Протоколы испытаний по ЭМС
81	№ ЕАС.04ИБН1.СМ.8045	Сертификат соответствия системы менеджмента качества изготовителя требованиям ГОСТ Р ИСО 9001-2015
82	-	Руководство по качеству
83	-	Порядок проведения входного контроля
84	-	Порядок внесения изменений в документацию
85	-	Правила внутреннего трудового распорядка

6. Термины, определения и сокращения используемые в отчёте

Функциональная безопасность (Functional Safety) **–** часть общей системы безопасности, обусловленная применением управляемого оборудования и системы управления и зависящая от правильности функционирования электрических/электронных/программируемых электронных систем, связанных с безопасностью, и других средств по снижению риска.

Отказобезопасность – свойства изделия, ориентированные на сохранение безопасности в случае отказа.

Электрическая/электронная/программируемая электронная система; Э/Э/ПЭ-система - система управления, защиты или мониторинга, основанная на использовании одного или нескольких Э/Э/ПЭ устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали данных и другие коммуникационные магистрали, исполнительные устройства и другие устройства вывода.

Отказ (failure) - прекращение способности функционального блока выполнять необходимую функцию либо функционирование этого блока любым способом, отличным от требуемого.

ДБО (SFF – safety fail fraction) **–** Доля Безопасных Отказов. Свойство элемента, связанного с безопасностью, определяемое отношением суммы средних частот безопасных отказов и опасных обнаруженных отказов к сумме средних частот безопасных и опасных отказов.

λsu – интенсивность необнаруженных безопасных отказов

λsd – интенсивность обнаруженных безопасных отказов

λdu – интенсивность необнаруженных опасных отказов.

λdd – интенсивность обнаруженных опасных отказов.

ОАС (HFT – hardware fault tolerance) **–** Отказоустойчивость Аппаратных Средств.

ОАС = X означает, что X+1 является минимальным числом отказов, которые могут привести к потере функции безопасности.

Средняя вероятность опасного отказа по запросу (probability of dangerous failure on demand,

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

PFDavg) – средняя неготовность Э/Э/ПЭ системы, связанной с безопасностью, обеспечить безопасность, т.е. выполнить указанную функцию безопасности, когда происходит запрос.

Средняя частота опасного отказа в час (average frequency of a dangerous failure per hour, **PFH**) – средняя частота опасного отказа Э/Э/ПЭ системы, связанной с безопасностью, выполняющей указанную функцию безопасности в течение заданного периода времени.

β – эффективность теста по выявлению опасных отказов.

Полнота безопасности (safety integrity) – вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного периода времени.

Полнота безопасности программного обеспечения - составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме и относящихся к программному обеспечению.

Полнота безопасности, касающаяся систематических отказов - составляющая полноты безопасности системы, связанной с безопасностью, касающаяся систематических отказов, проявляющихся в опасном режиме.

Полнота безопасности аппаратных средств - составляющая полноты безопасности системы, связанной с безопасностью, касающаяся случайных отказов аппаратуры, проявляющихся в опасном режиме.

УПБ (SIL – safety integrity level) – Уровень полноты безопасности: дискретный уровень (принимающий одно из четырёх значений), определяющий требования к полноте безопасности для функции безопасности, который ставится в соответствии с Э/Э/ПЭС системам, связанным с безопасностью.

7. Описание оборудования

Изделия выполняют функцию преобразователя измерительного или изолятора гальванического и используются в качестве разделительных элементов между искробезопасными и неискробезопасными цепями, обеспечивая безопасность работы приборов и датчиков, находящихся во взрывоопасных зонах.

Перечень изделий, на которые распространяется данный отчёт и их назначение указано в таблице 7.1

Таблица 7.1

Обозначение типа	Описание	Функция безопасности
Повторители сигналов искробезопасные ЛПА-310	Повторители сигналов искробезопасные ЛПА-310 предназначены для обеспечения искробезопасности цепей взрывозащищенных датчиков с унифицированным выходным сигналом постоянного тока 4…20 мА, подключаемых по двухпроводным линиям связи и размещаемых во взрывоопасной зоне.	Функцией безопасности является повторение действующего значения входного аналогового сигнала 4…20 мА в выходной аналоговый сигнал 4…20 мА с точностью не хуже 2% за время не более 20 мс
Барьеры искробезопасности ЛПА-340	Барьеры предназначены для питания, приема сигналов, преобразования сигналов и обеспечения искробезопасности электрических цепей первичных дискретных преоб-разователей, устанавливаемых во взрывоопасных зонах помещений и наружных установок.	Функция безопасности барьера состоит в корректном транслировании состояния входного состояния датчика на свой выход за время, не более 20 мс.
Преобразователи температуры вторичные Искробезопасные ЛПА-350	Преобразователи предназначены для приема, преобразования и линеаризации сигналов от термопреобразователей сопротивления (ТС) и термопар (ТП), сигналов сопротивления и напряжения постоянного тока, выдачи выходных унифицированных аналоговых сигналов, обеспечения связи по интерфейсу RS-485 (не относится к функции безопасности), а также для обеспечения искробезопасно-сти электрических цепей	Функцией безопасности является преобразование и линеаризация входного аналогового от ТС или ТП в выходной аналоговый сигнал 4…20 мА с точностью не хуже 2% за время не более 3-х циклов преобразования АЦП.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

	устройств, устанавливаемых во взрывоопасных зонах помещений и наружных установок	

Подробно Функции безопасности и их характеристики описаны в руководстве по безопасности на конкретное изделие.

Конструктивно, изделия выполнены в неразборных пластмассовых корпусах, состоящих из нескольких частей и с установленными внутри печатными платами.

Изделия имеют клеммные колодки для подключения внешних цепей. Схемы подключения назначение разъёмов указаны в эксплуатационной документации изготовителя.

8. Методика оценки функциональной безопасности и краткие требования

8.1 Методика оценки

Оценка функциональной безопасности предполагает оценку всех мер предотвращения отказов на этапе разработки устройства.

Оценка учитывает все требования серии стандартов ГОСТ Р МЭК 61508, за исключением требований, которые были признаны неприменимыми к данному оборудованию.

Оценка укрупнённо заключается в оценке аппаратной части устройства и программного обеспечения, используемого в оборудовании.

Оценка также включает в себя анализ существующих производственных процедур обеспечения качества, чтобы удостовериться в соблюдении требований системы качества и жизненного цикла согласно ГОСТ Р МЭК 61508.

В рамках оценки функциональной безопасности по стандартам ГОСТ Р МЭК 61508 были проверены следующие аспекты:

- Управление функциональной безопасностью, включая обучение и учет компетенции персонала, планирование управления функциональной безопасностью и управление модификациями;
- Процесс определения требований, методик и документирования спецификаций;
- Процесс проектирования, включая разрабатываемую документацию и используемые инструменты;
- Подтверждение соответствия, включая процедуры проверки разработки, планы и протоколы испытаний, процедуры производственных испытаний и документирование информации;
- Проверка соответствия заданным требованиям;
- Процесс изменения и модификации;
- Требования к монтажу, эксплуатации и техническому обслуживанию;
- Система качества производства;
- Конструкция изделия и соответствие аппаратной части заданным требованиям;
- Архитектура устройства и режимы отказов, описанные в отчете по результатам анализа отказов, их последствий и диагностики (FMEDA);
- Оценка программного обеспечения устройства, включая его разработку, тестирование и используемые инструменты.

8.2 Уровень оценки

Оценка оборудования производилась в соответствии со стандартами ГОСТ Р МЭК 61508 до уровня полноты безопасности УПБ 3 (SIL 3) для барьеров и повторителей ЛПА-310 и ЛПА-340 и до уровня полноты безопасности УПБ 2 (SIL 2) для преобразователей ЛПА-350.

Все методы и средства используемые в процессе разработки, а также необходимость их применения оценивалась как соответствующие УПБ 3 (SIL 3) для барьеров и повторителей ЛПА-310 и ЛПА-340 и УПБ 2 (SIL 2) для преобразователей ЛПА-350.

8.3 Описание требований к жизненному циклу.

Жизненный цикл системы безопасности должен соответствовать требованиям раздела 7 ГОСТ Р МЭК 61508-2-2012 с учетом обязательных приложений А и В. Методы и средства, применяемые при разработке жизненного цикла, должны соответствовать заявленному уровню полноты безопасности.

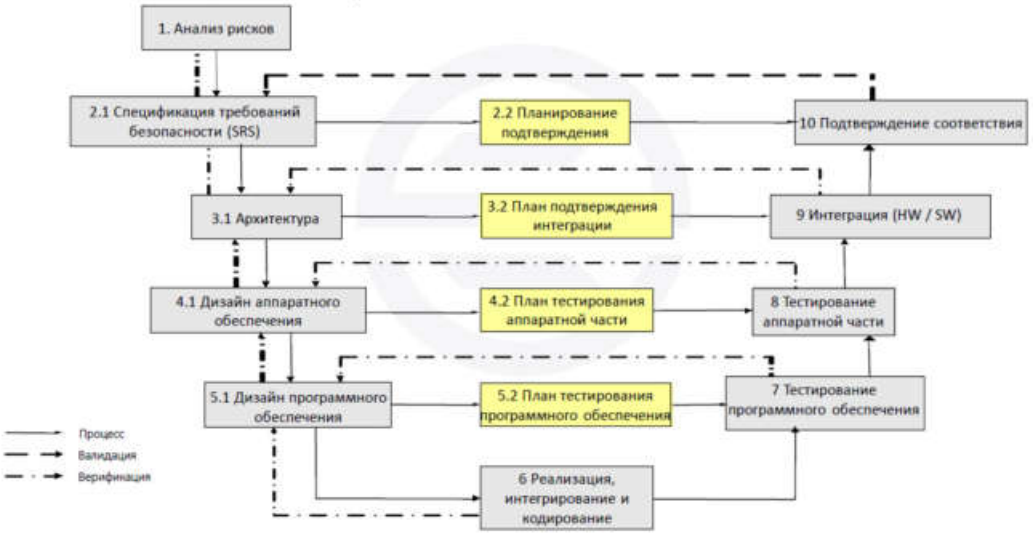
Жизненный цикл состоит из следующих этапов:

- Спецификация требований безопасности;
- Планирование подтверждения соответствия безопасности;
- Проектирование и разработка аппаратного обеспечения;

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

- Проектирование и разработка программного обеспечения;
- Тестирование аппаратного обеспечения;
- Тестирование программного обеспечения;
- Интеграция;
- Процедуры эксплуатации и технического обслуживания;
- Подтверждение соответствия безопасности;
- Модификация;
- Верификация.

Информация на всех этапах жизненного цикла должна быть документирована, должны быть указаны входы и выходы данного этапа, описаны цели и задачи.



Жизненный цикл безопасности (аппаратная часть и программное обеспечение)

Перечень методов и средств, применяемых на отдельных этапах жизненного цикла, для предотвращения систематических отказов, приведен в приложениях А (таблицы А.15-А.17) и В (таблицы В.1-В.5) ГОСТ Р МЭК 61508-2 и в ГОСТ Р МЭК 61508-7. Для каждого из них приведены рекомендации по необходимости применения для достижения Уровня Полноты Безопасности (SIL). Эти рекомендации обозначаются следующим образом:

М - данные методы или средства требуются обязательно (О) для данного уровня полноты безопасности;

HR - методы или средства крайне рекомендованы (КР) для данного уровня полноты безопасности. Если эти методы или средства не используются, то должно быть приведено подробное обоснование их неиспользования;

R - методы или средства рекомендованы (Р) для данного уровня полноты безопасности;

- - методы или средства, не имеющие рекомендаций за и против применения;

NR - методы или средства явно (положительно) не рекомендованы для данного уровня полноты безопасности. В случае применения этих методов или средств должно быть приведено подробное обоснование такого использования.

Требуемую эффективность методов и средств обозначают:

- "низкая (Low)" - данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня низкой эффективности противодействия систематическим отказам;

- "средняя (Medium)" - данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня средней эффективности противодействия систематическим отказам;

- "высокая (High)" - данные методы, меры или средства должны использоваться в степени, необходимой для достижения по крайней мере уровня высокой эффективности противодействия систематическим отказам.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

8.4 Описание требований к аппаратной части устройства.

Для соответствия аппаратной части необходимому уровню УПБ (SIL) должны выполняться требования к архитектурным ограничениям и вероятностным показателям отказов.

Наиболее высокий уровень полноты безопасности аппаратных средств, который может потребоваться для функции безопасности, ограничен предельными значениями полноты безопасности аппаратных средств, которые достигаются одним из двух возможных способов (реализуемых на уровне системы или подсистемы):

- способ 1н основан на концепции отказоустойчивости аппаратных средств и концепции, составляющей безопасных отказов;
- способ 2н основан на полученных данных о безотказности компонентов, об их использовании конечными пользователями, повышающих уровни доверия и отказоустойчивость аппаратных средств для указанных уровней полноты безопасности.

Величина ДБО (SFF) для способа 1н определяется по результатам Failure modes, effects, and diagnostic analysis (FMEDA). Методика и порядок оценки данным методом описан в Приложении С ГОСТ Р МЭК 61508-6-2012 и рассчитывается по формуле:

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$

Где,

λdd – интенсивность опасных детектируемых отказов;

λsd – интенсивность безопасных детектируемых отказов;

λsu – интенсивность безопасных недетектируемых отказов;

λdu – интенсивность опасных недетектируемых отказов.

Архитектурные требования к устройствам, связанным с безопасностью, изложены в ГОСТ Р МЭК 61508-2-2012 и приведены ниже.

Доля безопасных отказов (ДБО) для компонентов типа А.

Доля безопасных отказов	**Отказоустойчивость аппаратных средств**		
	N = 0	**N = 1**	**N = 2**
Менее 60%	УПБ 1	УПБ 2	УПБ 3
от 60% до менее 90%	УПБ 2	УПБ 3	УПБ 4
от 90% до менее 90%	УПБ 3	УПБ 4	УПБ 4
более и равно 99%	УПБ 3	УПБ 4	УПБ 4

Доля безопасных отказов (ДБО) для компонентов типа В.

Доля безопасных отказов	Отказоустойчивость аппаратных средств		
	N = 0	N = 1	N = 2
Менее 60%	не оговаривается	УПБ 1	УПБ 2
от 60% до менее 90%	УПБ 1	УПБ 2	УПБ 3
от 90% до менее 99%	УПБ 2	УПБ 3	УПБ 4
более и равно 99%	УПБ 3	УПБ 4	УПБ 4

Данная таблица в зависимости от значений ДБО (четыре диапазона значений) и отказоустойчивость аппаратных средств ОАС, устанавливает максимально обеспечиваемый данным устройством уровень УПБ (SIL) при применении метода 1н.

Величина отказоустойчивости аппаратных средств определяется в зависимости от канальной архитектуры подсистемы

Определение ОАС (HFT)

Канальная архитектура	**Отказоустойчивость аппаратных средств**
1oo1	0
1oo2	1
1oo3	2

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

2oo2	0
2oo3	1

Вероятностные требования к функции безопасности, изложены в ГОСТ Р МЭК 61508-1-2012, и приведены ниже.

Вероятностные требования

Уровень полноты безопасности	PFDavg	PFH
УПБ 4	$>10^{-5}$ - $<10^{-4}$	$>10^{-9}$ - $<10^{-8}$
УПБ 3	$>10^{-4}$ - $<10^{-3}$	$>10^{-8}$ - $<10^{-7}$
УПБ 2	$>10^{-3}$ - $<10^{-2}$	$>10^{-7}$ - $<10^{-6}$
УПБ 1	$>10^{-2}$ - $<10^{-1}$	$>10^{-6}$ - $<10^{-5}$

Для систем с архитектурой 1oo1 формула расчёта PFDavg имеет вид:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

Где MRT – среднее время ремонта в часах (обычно 8 часов);
MTTR – среднее время восстановления в часах (обычно 8 часов);
Ti – интервал времени между функциональными проверочными тестами (1–5–10 лет), обозначаемый также Tproof;
λdd – интенсивность опасных детектируемых отказов;
λdu – интенсивность опасных недетектируемых отказов

Для систем с архитектурой 1oo2 формула расчёта PFDavg имеет вид:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = 2\,((1-\beta_D)\lambda_{DD} + (1-\beta)\,\lambda_{DU})^2\, t_{GE}\, t_{CE}$$
$$+ \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

Где MRT – среднее время ремонта в часах (обычно 8 часов);
MTTR – среднее время восстановления в часах (обычно 8 часов);
TI – интервал времени между функциональными проверочными тестами (1–5–10 лет), обозначаемый также Tproof;
λdd – интенсивность опасных детектируемых отказов;
λdu – интенсивность опасных недетектируемых отказов
β – доля необнаруженных отказов, имеющих общую причину (выражается в виде доли в уравнениях и в процентах в других местах) (предполагается, что $\beta = 2 \times \beta_D$)
β_D – доля обнаруженных отказов, которые имеют общую причину
Коэффициент β определяется согласно приложению D ГОСТ Р МЭК 61508-6-2012
Охват диагностикой опасных отказов определяют с помощью следующего выражения

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{total}}$$

Для расчета PFH при архитектуре 1oo1 используют аналогичные значение частот отказов, а также значение t_{CE}

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Для систем с архитектурой 1oo1:

$$PFH_{1oo1} = \lambda_{DU}$$

Для систем с архитектурой 1oo2:

$$PFH_{1oo2} = 2 \cdot ((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU}$$

8.5 Описание требований к программному обеспечению устройства.

Разработка, испытание, верификация, и подтверждение соответствия программного обеспечения проводится в соответствии с ГОСТ IEC 61508-3-2018.

Согласно разделу 1 ГОСТ IEC 61508-3-2018 требования стандарта применяются к любому программному обеспечению, являющемуся частью системы, связанной с безопасностью, либо используемому для разработки системы, связанной с безопасностью. Такое программное обеспечение называется программным обеспечением, связанным с безопасностью.

Программное обеспечение, связанное с безопасностью, включает в себя операционные системы, системное программное обеспечение, программы, используемые в коммуникационных сетях, интерфейсы пользователей и обслуживающего персонала, встроенные программно-аппаратные средства, а также прикладные программы.

Согласно разделу 7 ГОСТ IEC 61508-3-2018 установлены требования к жизненному циклу разработки программного обеспечения.

Жизненный цикл разработки программного обеспечения выглядит следующим образом:

Жизненный цикл разработки ПО ГОСТ IEC 61508-3-2018 (отдельно от общего жизненного цикла)

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Перечень методов и средств, применяемых на отдельных этапах жизненного цикла программного обеспечения, приведен в приложениях А и В ГОСТ IEC 61508-3 и в ГОСТ Р МЭК 61508-7. Для каждого из них приведены рекомендации по необходимости применения для достижения Уровня Полноты Безопасности (SIL) программного обеспечения. Эти рекомендации обозначаются следующим образом:

Рекомендации по методам

HR	Настоятельно рекомендуется применять этот метод или средство для данного уровня полноты безопасности. Если этот метод или средство не используется, то на этапе планирования системы безопасности этому должно быть дано подробное объяснение со ссылкой на приложение С, и это объяснение должно быть согласованно с экспертом
R	Метод или средство рекомендуется применять для данного уровня полноты безопасности, но степень обязательности рекомендации ниже, чем в случае рекомендации HR
-	Для данного метода или средства рекомендации ни за ни против не приводятся
NR	Данный метод или средство не рекомендуется для этого уровня полноты безопасности. Если данный метод или средство применяют, то на стадии планирования системы безопасности этому должно быть дано подробное объяснение со ссылкой на приложение С, и это объяснение должно быть согласованно с экспертом.

Дополнительно ГОСТ IEC 61508-3-2018 разделяет программные средства, работающие в автономном режиме и неавтономном режиме. К средствам, работающим в неавтономном режиме (режиме реального времени), относятся операционная система реального времени, прикладные программы, коммуникационный софт. К такому программному обеспечению применяются все требования ГОСТ IEC 61508-3-2018. К средствам, работающим в автономном режиме, относятся средства поддержки проектирования (редактор кода, компилятор, среда программирования, средства тестирования, анализатор кода).

Средства поддержки программного обеспечения, работающие в автономном режиме можно разделить на следующие классы:

класс Т1 - не генерирует программ, которые явно или неявно включаются в рабочую программу (включая данные) системы, связанной с безопасностью.

Примечание -Примерами класса Т1 являются: текстовый редактор или средства поддержки проектирования, написанные не на автокоде;

класс Т2 - включает в себя средства тестирования или верификации проекта либо рабочей программы, причем такие, ошибки в которых могут привести к сбою при обнаружении ошибок в рабочей программе, но эти средства не могут создавать ошибки в самой рабочей программе.

Примечание -Примерами класса Т2 являются: генератор тестовых программ, средства измерения тестового охвата, средства статического анализа;

класс Т3 - генерирует программы, которые явно или неявно включаются в рабочую программу системы, связанной с безопасностью. Примерами класса Т3 являются: оптимизирующий компилятор, связь между исходным кодом программы и сгенерированным объектным кодом, которого не очевидна, компилятор, который включает исполнимый пакет программ в рабочую программу.

В зависимости от влияния средства поддержки программного обеспечения в автономном режиме на функцию безопасности, такое программное обеспечение относится к связанному с безопасностью.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

9. Результаты оценки функциональной безопасности

9.1 Процессы жизненного цикла изделия и меры предотвращения систематических отказов

В ходе оценки жизненного цикла изделий проверялось соответствие стандарту ГОСТ Р МЭК 61508 в части процессов, процедур и методов, используемых при проектировании и разработке заявленного изделия на соответствие уровню полноты безопасности УПБ 3.

В компании ООО "ЛЕНПРОМАВТОМАТИКА" внедрен процесс управления жизненным циклом изделия, что описано в руководстве по качеству, а также в плане управления функциональной безопасности.

Спецификации требований к оборудованию описаны в технических условиях, а также в отдельных спецификациях безопасности. Проведение испытаний изделия описано также в технических условиях, а также в отдельных методиках испытаний на соответствующие показатели. Также создаются планы безопасности, планы валидации и верификации.

Установленный процесс внесения изменений описан в документах по качеству.

Конструкция включает преобразователей температуры вторичных искробезопасных ЛПА-350 включает в себя программное обеспечение, которое также имеет необходимый жизненный цикл с применением обязательных методов для уровня УПБ 2. Подробный отчёт соответствия программного обеспечения приведён в разделе 9.3 данного отчёта.

9.1.1 Управление функциональной безопасностью

Планирование управления функциональной безопасностью

В компании реализован процесс проектирования и разработки изделий. Установлены обязательные требования к проектированию наряду с требованиями к проверке и испытаниям изделия. Это описано в технических условиях на продукцию, а также в спецификациях требований безопасности. Процесс внесения изменений описан в руководстве по качеству и отдельных документах по качеству. Данный процесс и входящие в него процедуры отвечают требованиям ГОСТ Р МЭК 61508.

Управление версиями

Внесение изменений в техническую документацию происходит в соответствии документами системе менеджмента качества.

Обучение, компетентность сотрудников

Управление персоналом описано в руководстве по качеству. Все сотрудники проходят периодическую подготовку и обучение в соответствии с занимаемыми должностями и производственной необходимостью. Сотрудники имеют знания и опыт работы со стандартами ГОСТ Р МЭК 61508.

9.1.2 Описание требований безопасности и проектирования.

Общие требования к конструкции изделия описаны в спецификациях требований безопасности. При создании устройства создаётся спецификация требований безопасности. Также создаются спецификации, рабочие чертежи, схемы, процедуры изготовления отдельных элементов и требования к производственной среде при изготовлении.

В процессе задания спецификаций используются методы управления проектами, управление документацией, структурирование спецификаций. Также применяются полуформальные методы. Согласно ГОСТ Р МЭК 61508-2-2012, Таблица В.1, данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 3.

Методы и средства по предотвращению ошибок во время формирования спецификации требований проектирования

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Управление проектами	О (М) средний	Применяется	УПБ 3
2 Документация	О (М) средний	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

3 Разделение Э/Э/ПЭ систем, связанных с безопасностью, и систем, не связанных с безопасностью	КР (HR) средний	Применяется	УПБ 3
4 Структурирование спецификации	КР (HR) средний	Применяется	УПБ 3
5 Экспертиза спецификации	КР (HR) средний	Применяется	УПБ 3
6 Полуформальные методы	КР (HR) средний	Применяется	УПБ 3
7 Таблица контрольных проверок	Р (R) низкий	Не применяются	УПБ 3
8 Автоматизированные средства разработки спецификаций	Р (R) низкий	Не применяются	УПБ 3
9 Формальные методы	Р (R) средний	Не применяются	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

9.1.3 Изготовление и разработка устройства

В процессе проектирования и изготовления устройства применяются методы соблюдения руководящих материалов и стандартов, управление проектами, документация, применяются полуформальные методы. Согласно ГОСТ Р МЭК 61508-2-2012, Таблица В.2, данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 3.

Методы и средства по предупреждению внесения ошибок во время проектирования и разработки

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Соблюдение руководящих материалов и стандартов	О (М) высокий	Применяются стандарты ГОСТ Р МЭК 61508	УПБ 3
2 Управление проектами	О (М) средний	Применяется	УПБ 3
3 Документация	О (М) средний	Применяется	УПБ 3
4 Структурное проектирование	КР (HR) средний	Применяется	УПБ 3
5 Модульное Проектирование	КР (HR) средний	Применяется (разнесение функционально значимых блоков на различных печатных платах)	УПБ 3
6 Использование достоверно испытанных компонентов	Р (R) средний	Применяются только проверенные компоненты	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

7 Полуформальные методы	КР (HR) средний	Применяется	УПБ 3
8 Таблица контрольных проверок	Р (R) средний	Не применяются	УПБ 3
9 Средства автоматизированного проектирования	Р (R) средний	Не применяются	УПБ 3
10 Моделирование	Р (R) средний	Не применяются	УПБ 3
11 Сквозной анализ или поверка аппаратных средств	Р (R) средний	Не применяются	УПБ 3
12 Формальные методы	Р (R) средний	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

9.1.4 Интеграция и подтверждение соответствия

Процесс подтверждения правильности описан в документах системы качества изготовителя таких как технические условия, программы-методики испытаний в процессе изготовления. Все устройства проходят приёмосдаточные испытания на заводе-изготовителе в объёме, установленном требованиями проекта.

В процессе испытаний проводится функциональное тестирование, управление проектом, документирование, испытания в условиях окружающей среды. Согласно ГОСТ Р МЭК 61508-2-2012, Таблица В.3, Таблица В.5 данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 3.

Методы и средства для предотвращения ошибок на стадии интеграции

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Функциональное тестирование	О (М) высокий	Применяется	УПБ 3
2 Управление проектами	О (М) средний	Применяется	УПБ 3
3 Документация	О (М) средний	Применяется	УПБ 3
4 Тестирование методом "черного ящика"	Р (R) средний	Не применяется	УПБ 3
5 Полевые испытания	Р (R) средний	Не применяется	УПБ 3
6 Статистическое тестирование	Р (R) средний	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Методы и средства по предотвращению ошибок при подтверждении соответствия безопасности

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Функциональное тестирование	КР (HR) высокий	Применяется	УПБ 3
2 Функциональные испытания в условиях окружающей среды	КР (HR) высокий	Применяется, климатические испытания	УПБ 3
3 Испытания на устойчивость к пиковым выбросам внешних воздействий	КР (HR) высокий	Применяется	УПБ 3
4 Испытание с введением неисправностей (при требуемом охвате диагностикой >= 90%)	КР (HR) высокий	Применяется	УПБ 3
5 Управление проектами	О (M) средний	Применяется	УПБ 3
6 Документация	О (M) средний	Применяется	УПБ 3
7 Статический анализ, динамический анализ, анализ отказов	Р (R) средний	Применяется	УПБ 3
8 Моделирование и анализ отказов	Р (R) средний	Не применяется	УПБ 3
9 Анализ наихудшего случая, динамический анализ и анализ отказов	средний	Не применяется	УПБ 3
10 Статический анализ и анализ отказов	Р (R) средний	Применяется	УПБ 3
11 Расширенное функциональное тестирование	КР (HR) средний	Применяется	УПБ 3
12 Тестирование методом "черного ящика"	Р (R) средний	Не применяется	УПБ 3
13 Испытание с введением неисправностей (при требуемом охвате диагностикой >= 90%)	Р (R) средний	Применяется	УПБ 3
14 Статистическое тестирование	Р (R) средний	Не применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

15 Испытания в наихудших случаях	P (R) средний	Не применяется	УПБ 3
16 Полевые испытания	P (R) средний	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

9.1.5 Проверка соответствия заданным требованиям

Для каждого этапа проектирования и изготовления установлены задачи, необходимые исходные и итоговые документы, а также процедуры контроля и испытаний. Данные методы являются достаточными для достижения требуемого уровня полноты безопасности УПБ 3.

9.1.6 Внесение изменений

Перед утверждением все изменения рассматриваются и анализируются на предмет их влияния на проект и функции безопасности. Все изменения оформляются документально, и соответствующая информация вносится в необходимую техническую и проектную документацию. На предприятии имеются отдельно разработанные документы системы менеджмента качества по внесению изменений в конструкцию изделий и техническую документацию. Данные методы являются достаточными для достижения требуемого уровня полноты безопасности УПБ 3.

9.1.7 Эксплуатационная документация

В состав эксплуатационной документации входят:

- Руководство по эксплуатации;
- Паспорт;
- Руководство по функциональной безопасности.

Руководство по функциональной безопасности совместно с руководством по эксплуатации соответствуют требованиям ГОСТ Р МЭК 61508-2-2012, Приложение D и содержит необходимую информацию:

- функциональную спецификацию выполняемых функций;
- идентификацию конфигурации аппаратных средств и программного обеспечения;
- ограничения на использование применяемого изделия;
- виды отказов применяемого изделия;
- предполагаемую интенсивность отказов;
- диагностический испытательный интервал.

Руководство по функциональной безопасности содержит информацию о частоте отказов, режимах отказов и предлагаемых контрольных испытаниях.

Инструкции по эксплуатации учитывают удобство для пользователей, удобство для технического обслуживания, руководство проектом, документальное оформление, ограниченные возможности эксплуатации и допуск к эксплуатации только квалифицированного персонала. Данные методы соответствуют требованиям ГОСТ Р МЭК 61508-2-2012, Таблица B.4 и данных методов достаточно для достижения требуемого уровня полноты безопасности УПБ 3.

Методы и средства по предотвращению ошибок и отказов в период эксплуатации и технического обслуживания

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Инструкции по эксплуатации и техническому обслуживанию	KP (HR) высокий	Применяется. Имеется руководство по безопасности.	УПБ 3
2 Удобство общения с пользователем	KP (HR) высокий	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

3 Удобство общения с обслуживающим персоналом	КР (HR) высокий	Применяется	УПБ 3
4 Управление проектами	О (M) средний	Применяется	УПБ 3
5 Документация	О (M) средний	Применяется	УПБ 3
6 Сокращение работ на стадии эксплуатации	КР (HR) средний	Применяется	УПБ 3
7 Защита от ошибок оператора	КР (HR) средний	Применяется	УПБ 3
8 Эксплуатация только квалифицированным оператором	Р (R) средний	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

9.1.8 Систематическая полнота безопасности. Управление отказами при проектировании, отказы, связанные с внешними нагрузками, отказы на стадии эксплуатации.

В процессе разработки устройства учтены обязательные требования по следующим аспектам систематических отказов:

- управления отказами, связанными с проектированием аппаратных средств;
- управления отказами, вызванными внешними нагрузками или влияниями;
- управления отказами на стадии эксплуатации.

Методы и средства управления систематическими отказами, источниками которых являются этапы разработки аппаратных средств

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Мониторинг последовательности выполнения программ	КР (HR) средний	Применяется для ЛПА-350. Остальные типы не имеют программного обеспечения	УПБ 3
2 Обнаружение отказов путем мониторинга в режиме онлайн	Р (R) средний	Применяется.	УПБ 3
3 Тестирование избыточными аппаратными средствами	Р (R) средний	Не применяется	УПБ 3
4 Стандартный тестовый порт доступа и архитектура граничного сканирования	Р (R) средний	Не применяется	УПБ 3
5 Кодовая защита	Р (R) средний	Не применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

6 Разнообразие аппаратных средств	P (R) средний	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

Методы и средства управления систематическими отказами, вызванными внешними нагрузками или влияниями

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Меры против пропадания напряжения, изменений напряжения, перенапряжения, низкого напряжения и других явлений, таких как изменение частоты переменного тока электропитания, которое может привести к опасному отказу	O (M) средний	Применяется (схемотехнические методы, переход в безопасное состояние).	УПБ 3
2 Разделение линий электрического питания и линий передачи информации	O (M)	Применяется гальваническое разделение	УПБ 3
3 Повышение устойчивости к электромагнитным воздействиям	O (M) средний	Применяется, фильтры ЭМС.	УПБ 3
4 Средства против физического воздействия окружающей среды (например, температуры, влажности, воды, вибраций, пыли, разъедающих веществ)	O (M) высокий	Применяется.	УПБ 3
5 Мониторинг последовательности выполнения программ	KP (HR) средний	Применяется для ЛПА-350. Остальные типы не имеют программного обеспечения.	УПБ 3
6 Меры против повышения температуры	KP (HR) средний	Применяется	УПБ 3
7 Пространственное разделение групповых линий	KP (HR) средний	Применяется (пространственное разнесены, гальваническое разделение).	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

8 Принцип реактивного тока (нет необходимости в непрерывном контроле для достижения или поддержки безопасного состояния УО)	P (R)	Не применяется	УПБ 3
9 Средства обнаружения обрывов и коротких замыканий в линиях передачи сигналов	P (R)	Применяется	УПБ 3
10 Обнаружение отказов путем мониторинга в режиме онлайн	P (R) средний	Применяется	УПБ 3
11 Тестирование избыточными аппаратными средствами	P (R) средний	Не применяется	УПБ 3
12 Кодовая защита	P (R) средний	Не применяется	УПБ 3
13 Передача неэквивалентных сигналов	P (R) средний	Не применяется	УПБ 3
14 Разнообразие аппаратных средств	P (R) средний	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

Методы и средства управления систематическими отказами при эксплуатации

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для заявляемого устройства.	Максимально достижимый уровень УПБ
1 Защита от модификаций	O (M) средний	Применяется	УПБ 3
2 Обнаружение отказов путем мониторинга в режиме онлайн	P (R) средний	Применяется	УПБ 3
3 Подтверждение ввода	P (R) средний	Не применяется	УПБ 3
4 Программирование с проверкой ошибок	O (M) средний	Применяется для ЛПА-350	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

Вывод по оценке жизненного цикла устройства: Процессы жизненного цикла изделия и меры предотвращения систематических отказов соответствуют требуемому уровню полноты безопасности УПБ 3 (SIL 3).

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

9.2 Результаты оценки случайных отказов аппаратной части устройства

9.2.1 Методика оценки

В соответствии с приложением С ГОСТ Р МЭК 61508-2-2012 Охват диагностикой и доля безопасных отказов элемента рассчитываются следующим образом:

a) проводят анализ видов отказов и их влияния для определения влияния каждого вида отказов каждого компонента или группы компонентов в элементе на поведение Э/Э/ПЭ систем, связанных с безопасностью, в отсутствие диагностических проверок.

b) все виды отказов делят на категории по признаку, является ли он (в отсутствие диагностических испытаний):
- безопасным отказом или
- опасным отказом;

c) отказы компонентов, не принадлежащих Э/Э/ПЭ системе, связанной с безопасностью, а также отказы, не влияющие на поведение Э/Э/ПЭ системы, связанной с безопасностью, не должны учитываться при вычислении охвата диагностикой (ОД) или доли безопасных отказов (ДБО);

d) оценив частоты отказов каждого компонента или группы компонентов и с учетом видов отказов и результатов анализа последствий каждого вида отказа каждого компонента или группы компонентов, вычисляют частоту безопасных отказов и частоту опасных отказов. Если одна из этих интенсивностей отказов не будет иметь постоянного значения, то необходимо оценить ее среднее число за конкретный период времени и использовать для вычислений ОД и ДБО;

e) оценивают для каждого компонента или группы компонентов доли опасных отказов, которые могут быть обнаружены диагностическими тестами и, следовательно, частоты опасных отказов, обнаруженных диагностическими тестами;

f) вычисляют полные частоты опасных отказов, полные частоты опасных отказов, обнаруженных диагностическими тестами, и полные частоты безопасных отказов;

g) вычисляют охват диагностикой элемента;

h) вычисляют долю безопасных отказов элемента.

При вычислении охвата диагностикой для элемента (см. приложение С.1 ГОСТ Р МЭК 61508-2-2012) для каждого компонента или группы компонентов необходимо оценить долю опасных отказов, обнаруживаемых диагностическими тестами. Диагностические тесты, которые могут внести вклад в охват диагностикой, включают в себя (но не ограничиваются) такие меры, как:

- сравнительные проверки, например контроль и сравнение избыточных (резервных) сигналов;
- дополнительные встроенные тестовые программы, например вычисление контрольных сумм в устройстве памяти;
- контроль с помощью внешних воздействий, например пропусканием импульсного сигнала через контролируемые тракты;
- непрерывный контроль аналогового сигнала, например для обнаружения выхода из диапазона уровней показаний при отказе сенсора.

Рекомендуемые методы и средства диагностического тестирования (испытания) и рекомендуемые максимальные диагностические охваты, которые могут потребоваться, приведены в таблицах А.2-А.14 ГОСТ Р МЭК 61508-2-2012. Эти тесты проводят непрерывно или периодически (в зависимости от интервала диагностического тестирования).

Для определения интенсивностей отказов и доли безопасных отказов специалистами ООО СЦ "Эндьюренс" совместно с изготовителем был выполнен **FMEDA** анализ устройства и проанализированы его результаты.

Анализ режимов отказов и их последствий (FMEA) — это системный способ определения и оценки влияния разных типов отказов компонентов, позволяющий понять, каким образом можно устранить или снизить вероятность отказа, а также документального описания архитектуры устройства.

Анализ режимов отказов, их последствий и диагностики (FMEDA) — это расширенная версия FMEA. Данный метод объединяет стандартные методы FMEA с дополнительными методами, чтобы определить способы диагностики и режимы отказов, относящиеся к выполнению функции безопасности устройства.

Следующие **исходные предпосылки** были сделаны при анализе видов, эффектов и диагностики отказов:

- Интенсивность отказов является постоянной величиной;
- Отказы, возникающие в процессе задания параметров не рассматриваются;
- Повторители сигналов искробезопасные ЛПА-310 и Барьеры искробезопасности ЛПА-340 относятся к компонентам типа А;

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

- Преобразователи температуры вторичные искробезопасные ЛПА-350 относятся к компонентам типа В;
- Отказом оборудования и модулей, входящих в состав, считается невозможность выполнения заявленных функций безопасности;
- Данные по интенсивности отказов взяты из Siemens Standard SN 29500 являющимся надежным источником;
- Приведенные интенсивности отказов соответствуют типичным условиям эксплуатации на промышленных предприятиях, описанным в стандарте МЭК 60654-1, класс С.

9.2.2 Сводные значения и результаты оценки случайных отказов аппаратной части.

Сводные значения результатов расчета показателей уровня полноты безопасности в части случайных отказов приведены в таблицах 9.1 и 9.2

Таблица 9.1

Модель / режим работы	Тип элемента	λsd, FIT	λsu, FIT	λdd, FIT	λdu, FIT	ДБО (SFF), %	УПБ (уровень полноты безопасности)
Повторители сигналов искробезопасные ЛПА-310							
ЛПА-310-200	Тип А	0	0	405	171	70,32	УПБ 2 (HFT=0); УПБ 3 (HFT=1)
ЛПА-310-100		0	0	403	171	70,25	
ЛПА-310-110 1oo1		0	0	818	182	81,80	
ЛПА-310-110 1oo2		107	1,08	898	84,6	92,24	УПБ 3 (HFT=1)
Барьеры искробезопасности ЛПА-340							
ЛПА-340-100 без различения ошибки (0000000)	Тип А	0	387,37	0	32,80	92,19	УПБ 3 (HFT=0)
ЛПА-340-100 без различения ошибки (0001000)		0	351,70	0	68,65	83,67	УПБ 2 (HFT=0); УПБ 3 (HFT=1)
ЛПА-340-100 подключение единым шлейфом с различением ошибки (0000000)		316,11	71,26	0	32,80	92,19	УПБ 3 (HFT=0)
ЛПА-340-100 подключение единым шлейфом с различением ошибки (0001000)		316,44	35,26	0	68,65	83,67	УПБ 2 (HFT=0); УПБ 3 (HFT=1)
ЛПА-340-100 подключение независимыми шлейфами с различением ошибки (0000000)		290,05	70,99	26,06	33,06	92,13	УПБ 3 (HFT=0)
ЛПА-340-100 подключение независимыми шлейфами с различением ошибки (0001000)		222,61	34,31	93,83	69,59	83,44	УПБ 2 (HFT=0); УПБ 3 (HFT=1)
ЛПА-340-220 (X0X0X00)		373,37	69,25	0	66,04	87,02	
ЛПА-340-220 (X0X1X00)		373,70	33,29	0	101,85	79,98	
Преобразователи температуры вторичные искробезопасные ЛПА-350							
ЛПА-350-220(221) ТС [3]	Тип В	0	0	774	73,0	91,38	УПБ 2 (HFT=0)
ЛПА-350-110(111) ТС [3]		0	0	702	72,3	90,67	
ЛПА-350-120(121) ТС [3] 1oo1		0	0	684	72,1	90,46	
ЛПА-350-120(121) ТС [3] 1oo2	Тип В	8,63	0	710	72,4	90,85	УПБ 2 (HFT=1)
ЛПА-350-220(221) ТП [4]		0	0	773	76,4	91,01	УПБ 2 (HFT=0)
ЛПА-350-110(111) ТП [4]		0	0	703	75,6	90,30	
ЛПА-350-120(121) ТП [4] 1oo1		0	0	685	75,4	90,08	
ЛПА-350-120(121) ТП [4] 1oo2		8,63	0	711	75,6	90,49	УПБ 2 (HFT=1)

[1] FIT = 1отказ/10^9 часов - единица измерения интенсивности отказов.

[2] Подробные режимы работы и схемы подключения приборов указаны в руководствах по безопасности.

[3] Преобразователь сконфигурирован в режим приема сигнала от термопреобразователей сопротивления.

[4] Преобразователь сконфигурирован в режим приема сигнала от термопар.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Таблица 9.2

Модель / режим работы	PFD_{avg}	PFH (1/час)
ЛПА-310-200	$7{,}54 \cdot 10^{-4}$	$1{,}71 \cdot 10^{-7}$
ЛПА-310-100	$7{,}54 \cdot 10^{-4}$	$1{,}71 \cdot 10^{-7}$
ЛПА-310-110 1oo1	$8{,}05 \cdot 10^{-4}$	$1{,}82 \cdot 10^{-7}$
ЛПА-310-110 1oo2	$3{,}78 \cdot 10^{-4}$	$8{,}46 \cdot 10^{-8}$
ЛПА-340-100 без различения ошибки (0000000)	$1{,}44 \cdot 10^{-4}$	$3{,}28 \cdot 10^{-8}$
ЛПА-340-100 без различения ошибки (0001000)	$3{,}01 \cdot 10^{-4}$	$6{,}87 \cdot 10^{-8}$
ЛПА-340-100 подключение единым шлейфом с различением ошибки (0000000)	$1{,}44 \cdot 10^{-4}$	$3{,}28 \cdot 10^{-8}$
ЛПА-340-100 подключение единым шлейфом с различением ошибки (0001000)	$3{,}01 \cdot 10^{-4}$	$6{,}87 \cdot 10^{-8}$
ЛПА-340-100 подключение независимыми шлейфами с различением ошибки (0000000)	$1{,}45 \cdot 10^{-4}$	$3{,}31 \cdot 10^{-8}$
ЛПА-340-100 подключение независимыми шлейфами с различением ошибки (0001000)	$3{,}06 \cdot 10^{-4}$	$6{,}96 \cdot 10^{-8}$
ЛПА-340-220 (X0X0X00)	$2{,}90 \cdot 10^{-4}$	$6{,}60 \cdot 10^{-8}$
ЛПА-340-220 (X0X1X00)	$4{,}47 \cdot 10^{-4}$	$1{,}02 \cdot 10^{-7}$
ЛПА-350-220(221) ТС [3]	$3{,}27 \cdot 10^{-4}$	$7{,}30 \cdot 10^{-8}$
ЛПА-350-110(111) ТС [3]	$3{,}23 \cdot 10^{-4}$	$7{,}23 \cdot 10^{-8}$
ЛПА-350-120(121) ТС [3] 1oo1	$3{,}22 \cdot 10^{-4}$	$7{,}21 \cdot 10^{-8}$
ЛПА-350-120(121) ТС [3] 1oo2	$3{,}23 \cdot 10^{-4}$	$7{,}24 \cdot 10^{-8}$
ЛПА-350-220(221) ТП [4]	$3{,}41 \cdot 10^{-4}$	$7{,}64 \cdot 10^{-8}$
ЛПА-350-110(111) ТП [4]	$3{,}37 \cdot 10^{-4}$	$7{,}56 \cdot 10^{-8}$
ЛПА-350-120(121) ТП [4] 1oo1	$3{,}36 \cdot 10^{-4}$	$7{,}54 \cdot 10^{-8}$
ЛПА-350-120(121) ТП [4] 1oo2	$3{,}37 \cdot 10^{-4}$	$7{,}56 \cdot 10^{-8}$

PFDavg и PFH всей системы с учетом избыточных архитектур, интервала контрольных испытаний, эффективности контрольных проверок, любой автоматической диагностики, среднего времени ремонта и конкретной частоты отказов всех элементов системы, включенных в SIF. Каждый элемент должен быть проверен на соответствие минимальным требованиям отказоустойчивости оборудования (HFT).

9.2.3 Выводы по оценке аппаратной части

В процессе FMEDA анализа проанализированы режимы отказов оборудования и их частоты отказов.

В результате FMEDA анализа выявлено соответствие устройств уровню полноты безопасности УПБ 2 (SIL 2) и УПБ 3 (SIL 3) при отказоустойчивости аппаратных средств ОАС (HFT) = 0 и ОАС (HFT) = 1.

Уровень полноты безопасности УПБ (SIL) всей инструментальной функции безопасности (SIF), в которой применяется изделие, должен быть проверен путем расчета PFH всей системы с учетом избыточных архитектур, интервала контрольных испытаний, эффективности контрольных проверок, любой автоматической диагностики, среднего времени ремонта и конкретной частоты отказов всех элементов системы, включенных в SIF. Каждый элемент должен быть проверен на соответствие минимальным требованиям отказоустойчивости оборудования (HFT).

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

9.3 Результаты оценки программного обеспечения.

9.3.1 Общие данные о программном обеспечении

Программное обеспечение применяется только в преобразователях температуры вторичных искробезопасных ЛПА-350 и является прикладной программой, которая выполняется микроконтроллером STM32.

ПО написано на языке С при использовании интегрированной среды разработки предлагаемой STM32CUBE IDE со встроенными стандартами кодирования, тестирования и компиляции.

Тип программного обеспечения	**Обозначение программного обеспечения**	**Автономный / не автономный режим**	**Класс программного обеспечения**	**Комментарий**
Среда программирования	STM32CUBE IDE	Автономный	T1-T3	Имеет широкий опыт применения, имеет сертификаты соответствия требованиям 61508.
Средства тестирования	STM32CUBE, cppcheck	Не автономный	T2	Имеют сертификат соответствия УПБ 2, поддерживает MISRA C
Компилятор	Arm Compiler	Автономный	T3	Имеет сертификат соответствия УПБ 2
Прикладное ПО	C	Не автономный	-	Оценка на соответствие ГОСТ IEC 61508-3-2018 в данном отчёте.

9.3.2 Спецификация требований к программному обеспечению системы безопасности

В ходе разработки программного обеспечения задаются спецификации требований к ПО. Составляется описание программного обеспечения и спецификация требований безопасности.

Методы спецификации требований к программному обеспечению системы безопасности

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства	Максимально достижимый уровень УПБ
1a Полуформальные методы	R	Не применяются	УПБ 2
1b Формальные методы	R	Не применяются	УПБ 3
2 Прямая прослеживаемость между требованиями к системе безопасности и требованиями к программному обеспечению системы безопасности	R	Не применяется	УПБ 2
3 Обратная прослеживаемость между требованиями к системе безопасности и предполагаемыми потребностями безопасности	R	Не применяется	УПБ 2
4 Компьютерные средства разработки спецификаций для поддержки перечисленных выше подходящих методов/средств	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Полуформальные методы

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Логические/ функциональные блок-схемы	R	Не применяются	УПБ 2
2 Диаграммы последовательности действий	R	Не применяются	УПБ 2
3 Диаграммы потоков данных	R	Не применяются	УПБ 3
4a Конечные автоматы/диаграммы переходов	R	Не применяются	УПБ 2
4b Моделирование во времени сетями Петри	R	Не применяются	УПБ 2
5 Модели данных сущность-связь-атрибут	R	Не применяются	УПБ 3
6 Диаграммы последовательности сообщений	R	Не применяются	УПБ 3
7 Таблицы решений и таблицы истинности	R	Не применяются	УПБ 2
8 UML-диаграммы	R	Не применяются	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

В процессе разработки программного обеспечения создаются спецификации требований программного обеспечения. Полуформальные методы не применяются. Применяется спецификация путём описания. Данных методов достаточно для соответствия уровню УПБ 2.

9.3.3 Планирование подтверждения соответствия безопасности системы для аспектов программного обеспечения

В процессе разработки программного обеспечения создаётся план контроля качества программного обеспечения. Применяемых методов достаточно для соответствия уровню полноты безопасности УПБ2.

9.3.4 Проектирование и разработка программного обеспечения: проектирование архитектуры программного обеспечения

В ходе разработки программного обеспечения обеспечиваются обязательные требования к проектированию архитектуры ПО. Выполняется модульный подход, используются только доверенные программные модули. Данных методов достаточно для соответствия уровню УПБ 2.

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Методы при проектировании и разработке программного обеспечения: проектирование архитектуры программного обеспечения

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Обнаружение ошибок	R	Не применяется	УПБ 2
2 Коды обнаружения ошибок	R	Не применяется	УПБ 2
4b Постепенное отключение функций	R	Не применяется	УПБ 2
7 Модульный подход	HR	Применяется	УПБ 3
8 Использование доверительных/ проверенных элементов программного обеспечения (при наличии)	HR	Применяется.	УПБ 3
9 Прямая прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и архитектурой ПО	R	Не применяется	УПБ 2
10 Обратная прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и архитектурой ПО	R	Не применяется	УПБ 2
11a Методы структурных диаграмм	HR	Применяется	УПБ 3
11b Полуформальные методы	R	Не применяется	УПБ 2
12 Автоматизированные средства разработки спецификаций и проектирования	R	Не применяется	УПБ 2
13a Циклическое поведение с гарантированным максимальным временем цикла	HR	Применяется	УПБ 3
13b Архитектура с временным распределением	HR	Не применяется, 13a	УПБ 3
13c Управление событиями с гарантированным максимальным временем реакции	HR	Не применяется, 13a	УПБ 3
14 Статическое выделение ресурсов	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Модульный подход

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Ограничение размера программного модуля	HR	Применяется	УПБ 3
2 Управление сложностью программного обеспечения	R	Применяется. Программное обеспечение является простым.	УПБ 3
3 Ограничение доступа/инкапсуляции информации	HR	Применяется	УПБ 3
4 Ограниченное число параметров/фиксированное число параметров подпрограммы	R	Не применяется	УПБ 2
5 Одна точка входа и одна точка выхода в каждой подпрограмме и функции	HR	Применяется	УПБ 3
6 Полностью определённый интерфейс	HR	Применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.5. Проектирование и разработка программного обеспечения: инструментальные средства поддержки и языки программирования

При проектировании программного обеспечения выбираются инструментальные средства поддержки соответствующие заданному уровню полноты безопасности. Для языков программирования применяются стандарты кодирования, для сокращения ошибок на этапе компиляции.

Проектирование и разработка программного обеспечения: инструментальные средства поддержки и языки программирования.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Выбор соответствующего языка программирования	HR	Применяется язык C	УПБ 3
2 Строго типизированные языки программирования	HR	Применяется подмножество C (MISRA-C)	УПБ 3
3 Подмножество языка	–	Применяется подмножество C	УПБ 3
4a Сертифицираванные средства и сертифицированные трансляторы	HR	Использовались сертифицированные средства	УПБ 3
4b Инструментальные средства, заслуживающие доверия на основании опыта использования	HR	Применяются инструментальные средства с большим опытом эксплуатации.	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
Итоговый достигнутый уровень УПБ			**УПБ 3**

9.3.6 Проектирование и разработка программного обеспечения: детальное проектирование (включает в себя проектирование системы программного обеспечения, проектирование модуля программного обеспечения и кодирование)

При проектировании программного обеспечения применяется модульный подход, применяются стандарты кодирования, применяются средства автоматизированного проектирования. Данных методов достаточно для соответствия уровню УПБ 2.

Методы проектирования и разработки программного обеспечения: детальное проектирование.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1a Методы структурных диаграмм	HR	Не применяются, применяются 1b	УПБ 3
1b Полуформальные методы	HR	Применяются	УПБ 3
1c Формальные методы проектирования и усовершенствования	R	Не применяется	УПБ 3
2 Средства автоматизированного проектирования	R	Не применяется	УПБ 2
3 Программирование с защитой	R	Не применяется	УПБ 2
4 Модульный подход	HR	Применяется	УПБ 3
5 Стандарты для проектирования и кодирования	HR	Применяется. Используются стандарты для C	УПБ 3
6 Структурное программирование	HR	Применяется	УПБ 3
7 Использование доверительных/ проверенных программных модулей и компонентов (по возможности)	HR	Применяется	УПБ 3
8 Прямая прослеживаемость между спецификацией требований к программному обеспечению системы безопасности и проектом программного обеспечения	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Стандарты для проектирования и кодирования

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Использование стандартов кодирования для сокращения вероятности ошибок	HR	Применяется	УПБ 3
2 Не использовать динамические объекты	HR	Применяется	УПБ 3
3a Не использовать динамические переменные	R	Не применяется	УПБ 2
3b Проверка создания динамических переменных в неавтономном режиме	R	Не применяется	УПБ 2
4 Ограниченное использование прерываний	R	Не применяется	УПБ 2
5 Ограниченное использование указателей	R	Не применяется	УПБ 2
6 Ограниченное использование рекурсий	R	Не применяется	УПБ 2
7 Не использовать неструктурированное управление в программах, написанных на языках высокого уровня	HR	Не используются	УПБ 3
8 Не использовать автоматическое преобразование типов	HR	Автоматическое преобразование типов не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.7. Проектирование и разработка программного обеспечения: тестирование и интеграция программных модулей

Методы тестирования и интеграции программных модулей включают динамический анализ и тестирование, функциональное тестирование методом чёрного ящика. Данных методов достаточно для соответствия уровню УПБ 2.

Методы тестирования и интеграции программных модулей.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1Вероятностное тестирование	R	Не применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
2 Динамический анализ и тестирование	HR	Применяется	УПБ 3
3 Регистрация и анализ данных	HR	Применяется	УПБ 3
4 Функциональное тестирование и тестирование методом черного ящика	HR	Применяется	УПБ 3
5 Тестирование рабочих характеристик	R	Не применяется	УПБ 2
6 Тестирование, основанное на модели	R	Не применяется	УПБ 2
7 Тестирование интерфейса	R	Применяется	УПБ 3
8 Управление тестированием и средства автоматизации	HR	Применяется	УПБ 3
9 Прямая прослеживаемость между спецификацией проекта программного обеспечения и спецификациями тестирования модуля и интеграции	R	Не применяется	УПБ 2
10 Формальная верификация	R	Не применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

Динамический анализ и тестирование

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Выполнение тестового примера, связанного с анализом граничных значений	HR	Применяется	УПБ 3
4 Выполнение тестового примера, сгенерированного на основе модели	R	Не применяется	УПБ 2

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
7a Структурный тест со 100-% охватом (точки входа)	HR	Применяется	УПБ 3
7a Структурный тест со 100-% охватом (операторы)	HR	Применяется	УПБ 3
7c Структурный тест со 100-% охватом (условные переходы)	HR	Применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ2**

Функциональное тестирование и проверка методом черного ящика

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
2 Выполнение тестового примера, сгенерированного на основе модели	R	Не применяется	УПБ 2
4 Разделение входных данных на классы эквивалентности, включая анализ граничных значений	HR	Применяется.	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 2**

Тестирование рабочих характеристик

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Проверка на критические нагрузки и стресс-тестирование	HR	Применяется	УПБ 3
2 Ограничение на время ответа и объём памяти	HR	Применяется	УПБ 3
3 Требования к реализации	HR	Применяется	УПБ 3
Итоговый достигнутый уровень УПБ			**УПБ 3**

9.3.8. Подтверждение соответствия безопасности системы аспектов программного обеспечения

Подтверждения соответствия аспектов программного обеспечения проводится с помощью

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

функционального тестирования, моделированная процесса. Данных методов достаточно для соответствия уровню УПБ 2.

Подтверждение соответствия ПО

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Вероятностное тестирование	R	Не применяется	УПБ 2
2 Моделирование процесса	R	Не применяется	УПБ 2
3 Моделирование	R	Не применяется	УПБ 2
4 Функциональное тестирование и тестирование методом черного ящика	HR	Применяется	УПБ 3
5 Прямая прослеживаемость между спецификацией требования к программному обеспечению и планом подтверждения соответствия программного обеспечения системы безопасности	R	Не применяется	УПБ 2
6 Обратная прослеживаемость между планом подтверждения соответствия программного обеспечения системы безопасности и спецификацией требования к программному обеспечению системы безопасности	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.9. Модификация программного обеспечения.

При модификации программных модулей проводится анализ влияния, повторное подтверждение соответствия аспектов ПО. Данных методов достаточно для соответствия уровню УПБ 2.

Модификация программного обеспечения

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Анализ влияния	HR	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
2 Повторная верификация измененных программных модулей	HR	Применяется	УПБ 3
3 Повторная верификация программных модулей на которые оказывают влияние изменения в других модулях	HR	Применяется	УПБ 3
4a Повторное подтверждение соответствия системы в целом	R	Не применяется	УПБ 2
4b Регрессионное подтверждение соответствия	HR	Применяется	УПБ 3
5 Управление конфигурацией программного обеспечения	HR	Применяется	УПБ 3
6 Регистрация и анализ данных	HR	Применяется	УПБ 3
7 Прямая прослеживаемость между спецификацией требования к программному обеспечению и планом модификации программного обеспечения системы безопасности	R	Не применяется	УПБ 2
6 Обратная прослеживаемость между планом модификации программного обеспечения системы безопасности и спецификацией требования к программному обеспечению системы безопасности	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.10. Верификация программного обеспечения

Верификация программного обеспечения (на отдельных этапах жизненного цикла) включает в себя методы статического анализа, динамическое тестирование. Данных методов достаточно для соответствия уровню УПБ 2.

Методы верификации программного обеспечения на различных этапах создания ПО.

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Формальное доказательство	R	Не применяется	УПБ 3
2 Анимация спецификации и тестирования	R	Не применяется	УПБ 3
3 Статический анализ	HR	Применяются статический анализатор, cppchek	УПБ 3
4 Динамический анализ и тестирование	HR	Применяется	УПБ 3

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
5 Прямая прослеживаемость между спецификацией проекта программного обеспечения и планом верификации программного обеспечения	R	Не применяется	УПБ 2
6 Обратная прослеживаемость между планом верификации и программного обеспечения и спецификацией проекта	R	Не применяется	УПБ 2
7 Численный анализ в автономном режиме	R	Не применяется	УПБ 2
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.10. Оценка функциональной безопасности.

Оценка функциональной безопасности программного обеспечения проводится путём составления контрольных проверок. Данных методов достаточно для соответствия уровню УПБ 2.

Оценка функциональной безопасности ПО

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
1 Таблица контрольных проверок	R	Не применяется	УПБ 3
2 Таблицы решений (таблицы истинности)	R	Не применяется	УПБ 3
3 Анализ отказов	R	Не применяется	УПБ 2
4 Анализ отказов по общей причине различного программного обеспечения (если используется различное программное обеспечение)	R	Не применяется	УПБ 2
5 Структурные схемы надежности	R	Не применяется	УПБ 3
6 Прямая прослеживаемость между требованиями раздела 8 и планом оценки функциональной безопасности программного обеспечения	R	Не применяется	УПБ 2

ООО Сертификационный центр «ЭНДЬЮРЕНС»
РФ, 115114, город Москва, 2-й Павелецкий проезд,
дом 5, строение 1, этаж 5, помещение VII, комната 11.
Телефон/факс: +7-495-799-07-93
сайт: https://www.ccendce.com, e-mail: info@ccendce.com

Метод/средство	Уровень необходимости применения метода для заявленного УПБ	Применяется/не применяется и интерпретация для программного обеспечения заявляемого устройства.	Максимально достижимый уровень УПБ
Итоговый достигнутый уровень УПБ			**УПБ 2**

9.3.11 Выводы по оценке программного обеспечения устройства

Программное обеспечение, используемое в преобразователях температуры вторичных искробезопасных ЛПА-350, соответствует требованиям к программному обеспечению, предъявляемым стандартом по функциональной безопасности ГОСТ Р МЭК 61508-3 для уровня полноты безопасности УПБ (SIL) = 2.

10. Заключение по результатам оценки

По результатам оценки повторителей сигналов искробезопасных ЛПА-310, барьеров искробезопасности ЛПА-340, преобразователей температуры вторичных искробезопасных ЛПА-350 можно сделать следующие краткие выводы:

- Процессы жизненного цикла изделия и меры предотвращения систематических отказов соответствуют требуемому уровню полноты безопасности УПБ 3 (SIL 3) для ЛПА-310, ЛПА-340 и УПБ 2 (SIL 2) для ЛПА-350.
- Аппаратная часть, частоты отказов, доля безопасных отказов, значения PFD и PFH соответствуют требованиям, предъявляемым к уровню полноты безопасности УПБ 2 (SIL 2) и УПБ 3 (SIL 3) при с учетом применяемых архитектур и условий избыточности аппаратных средств.

Уровень полноты безопасности УПБ (SIL) всей инструментальной функции безопасности (SIF), в которой применяются барьеры искрозащиты, должен быть проверен путем расчета PFDavg всей системы с учетом избыточных архитектур, интервала контрольных испытаний, эффективности контрольных проверок, любой автоматической диагностики, среднего времени ремонта и конкретной частоты отказов всех элементов системы, включенных в SIF. Каждый элемент должен быть проверен на соответствие минимальным требованиям отказоустойчивости оборудования (HFT).

- Программное обеспечение ЛПА-350 соответствует требования предъявляемым к уровню полноты безопасности УПБ 2 (SIL 2).

Повторители сигналов искробезопасные ЛПА-310, Барьеры искробезопасности ЛПА-340, соответствует требованиям, предъявляемым стандартами по функциональной безопасности для уровня полноты безопасности УПБ 2 (SIL 2) и УПБ 3 (SIL 3).

Преобразователи температуры вторичные искробезопасные ЛПА-350 соответствует требованиям, предъявляемым стандартами по функциональной безопасности для уровня полноты безопасности УПБ 2 (SIL 2) и УПБ 3 (SIL 3).

Отчёт составил:

Эксперт, Зубрев Е.О. _____ подпись «13» октября 2023 г.